2003 Security Plan Guidance, Attachment A

The following guidance contains numerous reminder of Cyber Security (CS) policy. These reminders are included in each section to assist each agency in more effectively completing the required plans this year. It is our intent to publish this material in our Cyber Security Manual, Series 3500, to provide a more permanent resource to use in the preparation of subsequent plans. We also updated this guidance with material from the following sources: NIST 800-12, Introduction to Cyber Security: The NIST Handbook; NIST 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems; NIST 800-16, Information Technology Security Training Requirements: A Role and Performance Based Model; NIST 800-18, Guide for Developing Security Plans for Information Technology Systems; NIST 800-26, Security Self-Assessment Guide for Information Technology Systems, NIST 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems (Draft) and NIST 800-50, Building an Information Technology Security Awareness and Training Program (Draft). In addition, Table A1 contains a list of Cyber Security Policy Guidance Memorandums and Directives on which this material is based.

The Agency Head or Administrator is responsible for ensuring that the security plan is developed, for implementing the plan and monitoring its effectiveness. Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," System Owners (SO), the System Administrator, and the System Security Manager.

If an agency has a contractor or other entity (e.g. state or local government) operating a system, they will be responsible for including the necessary contract language in procurement requests to specify compliance with the security plan in the development, maintenance and operation of all IT systems. Any security plan developed by a contractor or outside entity will always be reviewed and approved by the ISSPM and SO.

Determining General Support Systems and Major Applications:

All federal systems have some level of sensitivity and require protection as part of good management practice. The generic term "system" is used in this document to mean either a **major application** or a **general support system**. All applications and systems must be covered by system security plans if they are categorized as a "major application" or "general support system." Specific security plans for other applications are not required because the security controls for those applications or systems are provided by the general support systems in which they operate.

Each agency should begin by defining what constitutes a "system" which requires an analysis of system boundaries and organizational responsibilities. A system is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system must:

- Be under the **same** direct management control;

- Have the **same** function or mission objective;

- Have essentially the **same** operating characteristics and security needs; and

- Reside in the **same** general operating environment.

All components of a system need not be physically connected (e.g., [1] a group of stand-alone personal computers (PCs) in an office; [2] a group of PCs placed in employees' homes under defined telecommuting program rules; [3] a group of portable PCs provided to employees who require mobile computing capability for their jobs; and [4] a system with multiple identical configurations that are installed in locations with the same environmental and physical safeguards).

The next step is to categorize each system as either a "major application" or as a "general support system**.**" For example, a LAN may be designated a general support system and therefore requires a security plan. The organization's accounting system may be designated as a major application even though it is supported by the computing and communication resources of the LAN. In this example, the major application requires additional security requirements due to the sensitivity of the information the application processes. When a security plan is required for a major application that is supported by a general support system, coordination of both plans is required.

A **General Support System (GSS)** is interconnected information resources under the same direct management control which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a:

- LAN including smart terminals that support a branch office;

- Backbone (e.g., agency-wide);

- Communications network;

- Departmental data processing center including its operating system and utilities,

- Tactical radio network; or

- Shared information processing service organization.

A **Major Application (MA)** is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software and telecommunications components. Major applications can be either a major

software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

MAs can run on a general support system. The general support system plan should reference the major application plan(s) in Section 3.4, General Description/Purpose. All federal applications have value and require some level of protection and will be covered by a security plan. The applications will either be covered individually if they have been designated as a major application or within the security plan of a general support system. A system may be designated as a major application even though it is also supported by a system that has been designated as a general support system.

Agencies are expected to exercise management judgment in determining which of their applications qualify as MAs and to ensure that the security requirements of non-major applications are discussed as part of the security plan for the applicable general support systems.

As a reminder again, any system or applications not covered by a GSS or MA Plan will require its own specific plan. These plans will be prepared using the formats developed in Attachment B and will be retained by each agency staff for audit and review purposes. Only Overall Program Plan, GSS and MA Security Plans need to be submitted to Cyber Security.

Overall Program Plan Guidance:

MANAGEMENT CONTROLS

Management Controls are the organizational policies and procedures used by agencies to reasonably ensure that (1) programs achieve their intended results; (2) resources are used consistent with agency mission; (3) programs and resources are protected from waste, fraud, and mismanagement; (4) laws and regulations are followed; and (5) reliable and timely information is obtained, maintained, reported and used for decision making. In the broadest sense, they include the plan of the organization and methods or procedures adopted by management to ensure that its goals are met. Management controls include specific processes for planning, organizing, directing and controlling program operations.

A. ***Security Program Functions and Management Controls***: The purpose of a centralized Information Systems Security Program (ISSP) is to address the appropriate management of IT security within the USDA agency/mission area. Discuss the security management structure within the agency, including an organizational chart, showing the delegation of IT security authority through all layers of management to the Information Systems Security Program Manager (ISSPM) including field organizations. This section should address the current security management philosophy and specific functions of the ISSPM(s). Those duties include, but are not limited to, audits of system patches, personnel clearances, use of unauthorized or illegal software, incident response and reporting, change management procedures, security controls or as defined in DR 3140-1. Each agency will identify the responsible ISSPM and their deputies in writing. The scope

of the program in terms of the overall GSS and MA systems managed should be included. In addition, the specific security responsibilities of Field Security Officers should be outlined.

This section should also detail the Management Controls used to ensure that the agency meets its security goals. This includes internal controls used to assure that there is prevention or timely detection of unauthorized acquisition, use or disposition of the agencies' assets and taking timely and effective action to correct security deficiencies or weaknesses identified by the agency Information Systems Security Program Managers (ISSPM) in their oversight and monitoring responsibilities. Correcting these deficiencies is an integral part of management accountability and must be considered a priority by the agency. Discuss in detail how your agency uses management controls to protect information assets, ensure that systems are certified and accredited, conduct periodic reviews of information security procedures to ensure they work as intended and provide support for the role of the ISSPM in your organization.

B. ***Security Program:*** This section should discuss in specific detail the implementation of security policy and program activities. A key element of any successful security program is the evaluation of the sensitivity, confidentiality, integrity and availability of data. System *confidentiality* provides assurance that the information in an IT system is protected from disclosure to unauthorized persons, processes, or devices. System *integrity* provides assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. System *availability* provides assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service.

USDA organizations will evaluate the value and sensitivity of their data in terms of integrity, availability, and confidentiality. System criticality/sensitivity is a measure of the importance and nature of the information processed, stored, and transmitted by the IT system to the organization's mission and day-to-day operations. The criticality/sensitivity of an IT system and its information can be addressed by analyzing the system requirements for confidentiality, integrity, and availability.

By performing this analysis, the value of the system can be determined. The value is one of the major factors in risk management. Mission requirements also need to be considered. Table A2 at the end of this attachment provides guidance to agencies in assigning values to the levels of concern for confidentiality, integrity and availability. This portion of the plan should identify the assessments on which the determinations were made and policies created to meet the requirements. This evaluation will be reflected statistically (numerical representation of data) in the overall program plan and specifically in each system plan.

Describe your agency's process for the evaluation of data. In addition, identify, describe or clarify the policy that establishes and maintains the ISSP within the USDA agency, mission area or program. Include the specific internal ISSP policies issued during the past year and those being planned for the upcoming year. These can be policies, notices, or directives and should be noted by subject and date issued. Each agency will also generally discuss development of the Trusted Facilities Manual (TFM) and System Features Users Guide (SFUG) for all agency IT systems.

C. ***Long-Term Information System Security Strategy***: Identify and discuss long-term strategies to incorporate Information Systems Security (ISS) into the overall agency mission and into next generation of agency IT systems. The long-term Information Systems Security Program Strategy is based on the organizations:

- Policy Integration;
- Technology needs;
- Resource base and budget requirements;
- Security accomplishments/setbacks of the previous year;
- New initiatives (Telecommuting, PKI, VPN, E-Commerce, etc.,);
- Security goals and challenges for the upcoming year;
- Conformance to Departmental Architecture (Infrastructure/Security).

Each of these items should be described and documented in sufficient detail and clarity to define the organization's security program, policy, operations, management and oversight functions. Security Program Resource Base/Budget Requirements should cover detailed resource availability and plans for personnel, funds, and other support for the Security Program. Each agency will be required to submit an agency security budget as part of the A-11 IT budget process and enter security budget data into the Information Technology Investment Portfolio System (I-TIPS) as part of the annual IT budget request. Identification of resources for the ISS Program must include facilities, hardware, software, personnel, contract support, training, and any interagency commitments. The security plan must provide the foundation for linking security planning and activities from the Capital Planning and Investment Control (CPIC) and Government Information Security Reform Act (GISRA) now called the Federal Information Security Management Act (FISMA).

Figures determined as part of this process should match those contained in Attachment B, Overall Program Plan, includes a requirement to provide a copy of Figure 1, Cyber Security Program Operations costs, Figure 2, Major Security Initiatives Costs, and Figure 3, Physical Security Operations costs, if applicable, from the Information Technology Investment Portfolio System (I-TIPS) electronically.

D. ***Program Performance Measures:*** The Federal Information Security Management Act (FISMA), formerly called the Government Information Security Reform Act (GISRA), requires that each agency develop Performance Measures for their security program.

Performance measures are designed to be objective measures of how well the program performs in protecting agency assets. Describe in detail the Overall Performance Standards for the agency Security Program and how they are measured. If development of these measures is in process, provide an Action Plan with Milestones and target date (s) for completion of this project.

OMB memorandum M-01-24 outlines the following Performance Measure areas to be used to measure USDA's actual level of security performance:

- Risk Assessments
- Security Control Determination and Testing
- Updated Security Plans Used During System Life Cycle
- Agency Security Awareness and Training (General and Specific)
- Incident Response and FedCIRC Reporting
- Integration of Security into the CPIC Process
- Protection of Critical Assets in the Enterprise Architecture
- Audits and Inspections of Contractor Provided Services

E. ***Program Risk Assessment:*** Risk management addresses risks that arise from an organization's use of information technology. Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic steps: (1) determining the assessment's scope and methodology; (2) collecting and analyzing data; and (3) interpreting the risk analysis results. Risk assessments should be conducted for the overall agency security program.

Discuss the agency's security program risk assessment methodology. Include procedures in place for conducting a Program Risk Assessment, what approach is used, what type of documentation is maintained. In addition, summarize the Risk Assessment Report, vulnerabilities found and mitigation strategies. A risk management effort should focus on those areas that result in the greatest consequence to the organization (i.e., can cause the most harm). This effort should be done by ranking threats and assets. Risk mitigation involves the selection and the implementation of security controls used to reduce risk to a level acceptable to management. Discuss the selection of mitigations, timeframes for implementation, use of Risk Assessment Checklists and residual risk acceptance within your security program.

F. ***Certification and Accreditation Program***: The fundamental purpose of the certification process is to determine if the security controls for the IT system are appropriate, correctly implemented and are effective in their application. The correct and effective implementation of these controls provides assurance that the system security requirements have been satisfied.

There are three certification levels: Security Certification Level 1 (SCL-1), Security Certification Level 2 (SCL-2), and Security Certification Level 3 (SCL-3) as defined in NIST 800-37. Each of the successive certification levels provides additional rigor and intensity in

the application of the verification techniques to determine compliance with the security requirements and to demonstrate the correctness and effectiveness of the security controls. Use of the SCL will be based on the evaluation of data sensitivity, confidentiality, integrity and availability. Both the evaluation of data and the determination of the appropriate SCL must occur before systems are certified and accredited.

A formal Certification and Accreditation (C&A) Program is required for all agency IT systems regardless of where the system is in the life Cycle Process. Discuss the specifics your program for Certification and Accreditation of all agency IT systems. Note what stage the system is in and what efforts have been made toward C&A for the system. Outline what systems have not been formally certified and accredited and timeframes for completion.

G. ***Privacy***: The USDA recognizes that privacy protection is both a personal and fundamental right of its customers and employees as well as a requirement of law. Among the most basic of customers and employees' rights is an expectation that USDA will protect the confidentiality of personal, financial, and employment information. The Privacy Impact Assessment (PIA) is a process used to evaluate privacy in information systems. The PIA is designed to guide owners and developers in assessing privacy needs and protection requirements in the early stages of systems development. It is also used whenever a system undergoes a major change and should be considered in the C&A process. The PIA consists of privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks. Detail your agency efforts to implement privacy protection to include privacy training and number of Privacy Impact Assessments conducted.

H. ***Configuration Management:*** Configuration Management (CM) is a process of reviewing and controlling the components of an Information Technology System throughout its life cycle to ensure that they are well defined and cannot be changed without proper justification and full knowledge of the consequences. CM ensures that the hardware, software, communications services and documentation for a system can be accurately determined at any time.

Discuss the implementation of configuration management procedures and techniques within your agency. Identify your Agency Configuration Management (CM) Plan (Name, Date, Version). Provide the name of the Configuration Management Specialist (CMS) and describe the CM Plan used by field sites if not covered in the overall Agency CM Plan. Include information on the establishment of a Configuration Management Authority (CMA), Configuration Control Board (CCB) and the specific process used for change management during the Life Cycle of agency IT systems.

I. ***Compliance Program:*** A Compliance Program is designed to ensure that each agency reviews program security controls, policies and regulations on a regular basis, generally once a year. These reviews are a requirement of the Computer Security Act of 1987, and OMB Circular A-130, Appendix III. They include items such as the program Management Controls, Rules of Behavior, policies and procedures implemented, and security training. Security tends to degrade over time; these items are reviewed to ensure

that they are still operating effectively. Discuss in detail your agency's compliance program, who conducts reviews and how non-compliance is managed and corrected.

OPERATIONAL CONTROLS

These controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

A. ***Security Awareness and Training***: The Computer Security Act of 1987 and NIST 800-18 require that each agency provide security awareness and training. Additional guidance on how to build a Security Awareness and Training Program can be found in NIST 800-50 (Draft). The purpose of information systems security awareness and training is to enhance and improve knowledge concerning the need to protect system resources. Security training should also be designed to enhance agency employees, contractors, or other entity's knowledge to perform their jobs more effectively while reducing risk; and build an in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems. Training should specifically address an individual's role and responsibilities in relation to IT Security.

Specialized education, above the normal security training, is often required to ensure those system administrators and security personnel understand the security features of applications/systems. For example, security personnel may require training in Windows NT, UNIX Operating Systems, or security software for a particular system. This training is done in order to facilitate their understanding of how the security for various systems function and is part of a formal security training program. Plans for specialized training should be identified and included in the upcoming security budget and CPIC costs.

Discuss in upcoming agency specific plans for implementing an internal Security Awareness and Training Program. This program should include details on planned annual security seminars, use of electronic media, such as e-mail or bulletin boards to enhance security awareness, and plans for briefing new employees/contractors on security awareness. If your agency does not have an active security training and awareness program, provide specific details, including time frames, on your plans to meet this requirement. Provide specific information on the number of employees trained, type of training provided and date(s) of training. Also provide information on upcoming Security Training and Awareness efforts for the coming year. If your agency will be using training programs sponsored by the Department, explain your implementation approach for this training.

B. ***Security Clearances***: Federal and departmental regulations require that all competitive, executive, political appointment and contractor positions be reviewed and designated relative to the degree of harm the incumbent can do to the department's mission or national security based on access to information and assets.

Detailed information should be provided outlining the agency's policy and procedures for ensuring <u>all</u> positions have been reviewed for sensitivity level (Public Trust) and National

Defense clearance requirements. Include a statement as to whether all individuals working for the agency (federal employees as well as contractors) have received the appropriate background screening, suitability determination, and security clearance (if required) appropriate for the position to which they are assigned. At a minimum, all ISSPMs and their Deputies must have a completed background investigation to support a secret clearance.

Discuss in detail the requirement for National Defense Security Clearances at your agency and the policy and procedures in place to ensure appropriate background checks and reinvestigations are conducted, clearances are granted and security briefings given. Provide information on the number and level of security clearances required and granted at your agency. Include information on the number of pending background investigations.

Provide detailed information on policies and procedures in place if employee/contractor access is granted to systems and information before completion of the background check and suitability determination or security clearance and monitoring procedures for these employees to ensure that they do not gain access to sensitive or classified information. Discuss in detail policy and procedures for requesting, establishing, issuing, and closing user accounts.

C. ***Computer Incident Response Procedures***: The security of critical IT resources requires not only adopting reasonable precautions for securing these systems and networks, but also the ability to respond quickly and efficiently if the system or network security defenses are breached. A rapid and effective incident handling capability can be viewed as a component of contingency planning as it provides the ability to react quickly and efficiently to disruptions in normal agency data processing.

Discuss your ISS program's incident handling strategy and the internal procedures developed to support DM 3500-1, Chapter 1, USDA Computer Incident Response Procedures. Address centralized reporting, communications procedures, emergency points of contact, reporting requirements and the agency technical support for incident handling.

D. ***Contingencies and Disasters:*** A contingency plan is developed to cover potential disasters such as: power outages, hardware failures, fires, or storms; terrorist attacks, malicious intent to destroy or deny information or access; or unintentional mistakes that affect the system. Contingency planning directly supports an organization's goal of continued operations. Disaster plans should always address disaster recovery metrics such as the value of the assets, the amount of time a business can be without the system, the speed of processing, and storage capability at a minimum. Disaster Recovery Plans are prepared for the overall program and for all IT systems.

Discuss your Program contingency planning process to include: (1) identifying the mission, business, or critical functions; (2) identifying the resources that support the critical functions; (3) selecting contingency planning strategies; (4) anticipating potential

contingencies or disasters; (5) analyzing vulnerabilities and risks, and (6) physical and environmental security. Information should also be included on Business Resumption Plan and Contingency of Operations Plan (COOP). Also include a schedule for periodic testing of capability to perform the agency function supported by any application in the event of failure of its automated support**.** This testing process is also referred to as Continuity of Support and is required by OMB Circular A-130.

TECHNICAL CONTROLS

These controls consist of hardware or software used to provide automated protection to the system or applications. Technical controls operate within the technical system or applications.

A. ***Security Tools:*** Security tools have been proven to provide effective security protection when properly deployed and used as part of a comprehensive security process. The following are the most common types of security tools:

1. Intrusion Detection System (IDS): An Intrusion Detection System (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break in or compromise a system. An IDS differs from a firewall in that a firewall looks our for intrusions in order to stop them from happening. An IDS evaluates a suspected intrusion once it has taken place and sends an alarm. Discuss the use of Intrusion Detection Systems (IDS) within your agency with emphasis on what events or sequences of events are tracked and analyzed. If IDS is provided by another source, discuss how the events are used in your overall incident process.

2. Vulnerability Scanning: This is the automated process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Discuss your agency's use of vulnerability scanning software, frequency of use, outline whether this is provided by the department or another entity, the vulnerabilities uncovered and how these flaws are corrected. Cyber Security Guidance Memo, CS-007, dated 9/5/01, provides additional information on scanning.

3. Firewalls: This is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. Discuss

the use of firewalls in your agency, those provided by other sources such at the backbone network, and the frequency of firewall control settings reviews.

4. Anti-virus Program: This is commercial software that searches a hard disk or other media for known viruses and removes any that are found. Most anti-virus programs include an auto-update feature that enables the program to download profiles of new viruses as soon as they are discovered. Discuss anti-virus programs used in your agency, frequency of updates, equipment protected by these programs, and what software is being used for scanning (Departmental Scanner Software or other).

5. Encryption: Encryption methods protect sensitive information during storage and transmission. They provide important functionality to reduce the risk of intentional and accidental compromise and alteration of data. Discuss the use of encryption methods in your agency with emphasis on where encryption is deployed to protect Sensitive Security Information (SSI) or Sensitive But Unclassified (SBU) information. If encryption is utilized in a GSS, this protection method must be detailed in the system specific plan.

General Support System (GSS) Security Plan:

3.2 SYSTEM IDENTIFICATION

Date:

3.2.1 System Name/Title
Unique Identifier and Name Given to the System

3.2.2 Responsible Organization
List organization responsible for the system

3.2.3 Information Contact(s)
Name of person(s) knowledgeable about, or the owner of, the system.

- Name
- Title
- Address
- Phone

3.2.4 Assignment of Security Responsibility
Provide the name of person who has been designated in writing as responsible for security of the system.

- Name
- Title

- Address
- Phone

3.3 System Operational Status

Provide details with timeframes for portions of the system that are Under Development or Undergoing Major Modifications.

- Operational
- Under Development
- Undergoing a major modification

3.4 General Description/Purpose

- Describe the function or purpose of the system and the information processed.
- Describe the processing flow of the application from system input to system output.
- List user organizations (internal and external) and type of data and processing provided.
- List all applications supported by the general support system. Describe each application's functions and information processed.

3.5 System Environment

- Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)
- Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
- Include any security software protecting the system and information.

3.6 System Interconnection/Information Sharing

- List of interconnected systems and system identifiers (if appropriate).
- If connected to an external system not covered by a security plan, provide a short discussion of any security concerns that need to be considered for protection.
- It is required that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems. A description of these rules must be included with the security plan or discussed in this section.

3.7 SENSITIVITY OF INFORMATION HANDLED

3.7.1 Applicable Laws or Regulations Affecting the System

- List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.

3.7.2 General Description of Information Sensitivity

- Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: **High, Medium, or Low**.
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

3.8 CONFIGURATION MANAGEMENT INFORMATION

- Identify the Configuration Management Plan for this system (Name, Date and Version of the document). Is there a separate CCB Charter for this system (Yes or No)? Provide the names of the Configuration Control Authority (CCA), Configuration Management Authority and the Designated Accrediting Authority (DAA).

4 MANAGEMENT CONTROLS

4.1 Risk Assessments and Management

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

4.1.a Performance Measures

- Performance measures should be established around criteria such the Level of System Compromises, Timeliness of User Administration and Overall System Availability or other measures that reflect system security. Detail what performance measures are in place for this system.

4.2 Review of Security Controls

- Have there been major changes or upgrades to the system in the current year. If so, list any independent security reviews conducted on the system.
- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

4.3 Rules of Behavior

- A set of rules of behavior in writing must be established for each system. The rules of behavior should be made available to every user prior to receiving access to the system. It is recommended that the rules contain a signature page to acknowledge receipt.

- The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should state the consequences of inconsistent behavior or noncompliance. They should also include appropriate limits on interconnections to other systems.
- Attach the rules of behavior for the system as an appendix and reference the appendix number in this section or insert the rules into this section.

4.4 Planning for Security in the Life Cycle

Determine which phase(s) of the life cycle the system or parts of the system are in. Describe how security has been handled in the life cycle phase(s) that the system is currently in.

4.4.1 Initiation Phase

- Reference the sensitivity assessment that is described in Section 3.7, Sensitivity of Information Handled.

4.4.2 Development/Acquisition Phase

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

4.4.3 Implementation Phase

- Were design reviews and systems tests run prior to placing the system in production? Were the tests documented? Has the system been certified?
- Have security controls been added since development?
- Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?
- Include the date of the certification and accreditation. If the system is not authorized yet, include date when accreditation request will be made.

4.4.4 Operation/Maintenance Phase

- The security plan documents the security activities required in this phase.

4.4.5 Disposal Phase

- Describe in this section how information is moved to another system, archived, discarded, or destroyed. Discuss controls used to ensure the confidentiality of the information.

- Is sensitive data encrypted?
- How is information cleared and purged from the system?
- Is information or media purged, overwritten, degaussed or destroyed?

4.5 Authorize Processing

4.5.1 Certification and Accreditation

- Provide the date of system certification and accreditation, name, and title of management official authorizing processing in the system.
- If not authorized, provide the name and title of manager requesting approval to operate and date of request. Include information on an formal Interim Accreditation including planned certification and accreditation date.

4.5.2 Privacy

- Detail information on conducting the Privacy Impact Assessment (PIA) including date conducted. If not conducted, provide planned date.

5 GSS OPERATIONAL CONTROLS

5.GSS.1 Personnel Security

- Have all positions been reviewed for sensitivity level?
- Have individuals received background screenings appropriate and designated for the position to which they are assigned?
- Have all positions been reviewed and designated for a risk level?
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?
- Have security clearances been granted where appropriate? If not please explain what actions have been taken by the agency to follow up on the request.

5.GSS.2 Physical and Environmental Protection

- Discuss the physical protection for the system. Describe the area where processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.)
- Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems.

5.GSS.3 Production, Input/Output Controls

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, software should be listed. In this section, provide a synopsis of the procedures

in place that support the system. Below is a sampling of topics that should be reported in this section.

- User support - Is there a help desk or group that offers advice?
- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media
- Audit trails for receipt of sensitive inputs/outputs
- Procedures for restricting access to output products
- Procedures and controls used for transporting or mailing media or printed output
- Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary)
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)
- Audit trails for inventory management
- Media storage vault or library-physical, environmental protection controls/procedures
- Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing)
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse
- Procedures for shredding or other destructive measures for hardcopy media when no longer required

5.GSS.4 Contingency Planning

Describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster were to occur. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix. The procedure description should include:

- Any agreements of backup processing
- Documented backup procedures in including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)
- Location of stored backups and generations of backups kept
- Are tested contingency/disaster recovery plans in place? How often are they tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

5.GSS.5 Hardware and System Software Maintenance Controls

- Restriction/controls on those who perform maintenance and repair activities.
- Special procedures for performance of emergency repair and maintenance.

- Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).
- Procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.
- Version control that allows association of system components to the appropriate system version.
- Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.
- Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software.
- Change identification, approval, and documentation procedures.
- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.
- Are test data "live" data or made-up data?.
- Are there organizational policies against illegal use of copyrighted software or shareware?

5.GSS.6 Integrity Controls

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
- Is reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Is password crackers/checkers used?
- Is integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
- Are intrusion detection tools installed on the system?
- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?
- Is message authentication used in the system to ensure that the sender of a message is known and that the message has not been altered during transmission?

5.GSS.7 Documentation

Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security of the system to include backup and contingency activities, as well as descriptions of user and operator procedures.

- List the documentation maintained for the system (vendor documentation of hardware/software, functional requirements, security plan, program manuals, test results documents, standard operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, authorization for processing, verification reviews/site inspections).

5.GSS.8 Security Awareness & Training

- The awareness program for the system (posters, booklets, and trinkets)
- Type and frequency of general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training)
- The procedures for assuring that employees and contractor personnel have been provided adequate training

5.GSS.9 Incident Response Capability

- Are there procedures for reporting incidents handled either by system personnel or externally?
- Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?
- Who receives and responds to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?
- What preventative measures are in place, i.e., intrusion detection tools, automated audit logs, penetration testing?

6.GSS TECHNICAL CONTROLS

6.GSS.1.1 Identification and 6.GSS.1.2 Authentication

- Describe the method of user authentication (password, token, and biometrics).
- If a password system is used, provide the following specific information:
- Allowable character set;
- Password length (minimum, maximum);
- Password aging time frames and enforcement approach;
- Number of generations of expired passwords disallowed for use;
- Procedures for password changes;
- Procedures for handling lost passwords, and
- Procedures for handling password compromise.
- Procedures for training users and the materials covered.
- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).
- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.
- Describe any token controls used on this system and how they are implemented.

- Describe the level of enforcement of the access control mechanism (network, operating system, and application).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).
- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).
- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.
- If digital signatures are used, the technology must conforms with FIPS 186, *Digital Signature Standard* and FIPS 180-1, *Secure Hash Standard* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures.

6.GSS.2 Logical Access Controls

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists (ACLs).
- How are access rights granted? Are privileges granted based on job function?
- Describe the system's capability to establish an ACL or register.
- Describe how users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent user from accessing the system or applications outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.

- Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Dept. of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

6.GSS. 3 Audit Trails

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (type of event, when the event occurred, user id associated with the event, program or command used to initiate the event.)
- Is access to online audit logs strictly enforced?
- Is the confidentiality of audit trail information protected if, for example, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are guidelines.
- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?

Major Application Security Plan:

3.2 SYSTEM IDENTIFICATION

Date:

3.2.1 System Name/Title
Unique Identifier & Name Given to the System

3.2.2 Responsible Organization
List organization responsible for the application

3.2.3 Information Contact(s)
Name of person(s) knowledgeable about, or the owner of, the system.

- Name
- Title
- Address
- Phone

3.2.4 Assignment of Security Responsibility

Provide the name of person who has been designated in writing as responsible for security of the system.

- Name
- Title
- Address
- Phone

3.3 System Operational Status

Provide details with timeframes for portions of the system that are Under Development or Undergoing Major Modifications.

- Operational
- Under Development
- Undergoing a major modification

3.4 General Description/Purpose

- Describe the function or purpose of the application and the information processed.
- Describe the processing flow of the application from system input to system output.
- List user organizations (internal & external) and type of data and processing provided.

3.5 System Environment

- Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)
- Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
- Include any security software protecting the system and information.

3.6 System Interconnection/Information Sharing

- List interconnected systems and system identifiers (if appropriate).
- If connected to an external system not covered by a security plan, provide a short discussion of any security concerns that need to be considered for protection.
- **It is required that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems. A description of these rules must be included with the security plan or discussed in this section.**

3.7 SENSITIVITY OF INFORMATION HANDLED

3.7.1 Applicable Laws or Regulations Affecting the System

- List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.

3.7.2 General Description of Information Sensitivity

- Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: **High, Medium, or Low**.
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

3.8 CONFIGURATION MANAGEMENT INFORMATION

- Identify the Configuration Management Plan for this system (Name, Date and Version of the document). Is there a separate CCB Charter for this system (Yes or No)? Provide the names of the Configuration Control Authority (CCA), Configuration Management Authority and the Designated Accrediting Authority (DAA).

4 MANAGEMENT CONTROLS

4.1 Risk Assessment and Management

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

4.1.a Performance Measures

- Performance measures should be established around criteria such Data Integrity, Access to Application (unauthorized access attempts) or other measures that reflect application security. Detail what performance measures are in place for this application.

4.2 Review of Security Controls

- Have there been major changes or upgrades to the application in the current year. If so, list any independent security reviews conducted on the application.
- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

4.3 Rules of Behavior

- A set of rules of behavior in writing must be established for each system. The rules of behavior should be made available to every user prior to receiving access

to the system. It is recommended that the rules contain a signature page to acknowledge receipt.

- The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should state the consequences of inconsistent behavior or non-compliance. They should also include appropriate limits on interconnections to other systems.
- Attach the rules of behavior for the system as an appendix and reference the appendix number in this section or insert the rules into this section.

4.4 Planning for Security in the Life Cycle

Determine which phase(s) of the life cycle the system, or parts of the system are in. Describe how security has been handled in the life cycle phase(s) the system is currently in.

4.4.1 Initiation Phase

- Reference the sensitivity assessment that is described in Section 3.7, Sensitivity of Information Handled.

4.4.2 Development/Acquisition Phase

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

4.4.3 Implementation Phase

- Were design reviews and systems tests run prior to placing the system in production? Were the tests documented? Has the system been certified?
- Have security controls been added since development?
- Has the application undergone a technical evaluation to ensure that it meets
- applicable federal laws, regulations, policies, guidelines, and standards?
- Include the date of the certification and accreditation. If the system is not authorized yet, include date when accreditation request will be made.

4.4.4 Operation/Maintenance Phase

- The security plan documents the security activities required in this phase.

4.4.5 Disposal Phase

Describe in this section how information is moved to another system, archived, discarded, or destroyed. Discuss controls used to ensure the confidentiality of the

information.

- Is sensitive data encrypted?
- How is information cleared and purged from the system?
- Is information or media purged, overwritten, degaussed or destroyed?

4.5 Authorize Processing

4.5.1 Certification and Accreditation

- Provide the date of system certification and accreditation, name, and title of management official authorizing processing in the system.
- If not authorized, provide the name and title of manager requesting approval to operate and date of request. Include information on an formal Interim Accreditation

4.5.2 Privacy

- Detail information on conducting the Privacy Impact Assessment (PIA) including date conducted for this application.

5MA OPERATIONAL CONTROLS

5.MA.1 Personnel Security

- Have all positions been reviewed for sensitivity level?
- Have individuals received background screenings appropriate for the position to which they are assigned.
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?

5.MA.2 Physical and Environmental Protection

- Discuss the physical protection in the area where application processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.)
- Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems.

5.MA.3 Production, Input/Output Controls

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, application software should be listed. In this section, provide a synopsis of the procedures in place that support the operations of the application. Below is a sampling of topics that should be reported in this section.

- User Support - Is there a help desk or group that offers advice and can respond to security incidents in a timely manner? Are there procedures in place documenting how to recognize, handle, and report incidents and/or problems?
- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media
- Audit trails for receipt of sensitive inputs/outputs
- Procedures for restricting access to output products
- Procedures and controls used for transporting or mailing media or printed output
- Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary)
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)
- Audit trails for inventory management
- Media storage vault or library-physical, environmental protection controls/procedures
- Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing)
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse
- Procedures for shredding or other destructive measures for hardcopy media when no longer required

5.MA.4 Contingency Planning

Briefly describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix.

- Include descriptions for the following:
  - Any agreements of backup processing
  - Documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)
  - Location of stored backups and generations of backups
- Are tested contingency/disaster recovery plans in place? How often are they tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?
- Coverage of backup procedures, e.g., what is being backed up?

5.MA.5 Application Software Maintenance Controls

- Was the application software developed in-house or under contract?
- Does the government own the software? Was it received from another agency?

- Is the application software a copyrighted commercial off-the-shelf product or shareware? Has it been properly licensed and enough copies purchased for all systems?
- Is there a formal change control process in place and if so, does it require that all changes to the application software be tested and approved before being put into production?
- Are test data live data or made-up data?
- Are all changes to the application software documented?
- Are test results documented?
- How are emergency fixes handled?
- Are there organizational policies against illegal use of copyrighted software, shareware?
- Are periodic audits conducted of users computers to ensure only legal licensed copies of software are installed?
- What products and procedures are used to protect against illegal use of software?
- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

5.MA.6 Data Integrity/Validation Controls

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
- Is reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Is password crackers/checkers used?
- Is integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
- Are intrusion detection tools installed on the system?
- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- **Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?**
- Is message authentication used in the application to ensure that the sender of a message is known and that the message has not been altered during transmission?

5.MA.7 Documentation

Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support systems(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures.

- List the documentation maintained for the application (vendor documentation of hardware/software, functional requirements, security plan, general system security plan, application program manuals, test results documents, standard

operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, certification/accreditation statements/documents, verification reviews/site inspections.)

5.MA.8 Security Awareness and Training

- Describe the awareness program for the application (posters, booklets, and trinkets).
- Describe the type and frequency of application-specific and general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training).
- Describe the procedures for assuring that employees and contractor personnel have been provided adequate training.

6.MA TECHNICAL CONTROLS

6.MA.1.1 Identification and 6.MA.2.1 Authentication

- Describe the major application's authentication control mechanisms.
- Describe the method of user authentication (password, token, and biometrics)
- Provide the following if an additional password system is used in the application:
  - password length (minimum, maximum)
  - allowable character set,
  - password aging time frames and enforcement approach,
  - number of generations of expired passwords disallowed for use
  - procedures for password changes (after expiration and forgotten/lost)
  - procedures for handling password compromise

- Indicate the frequency of password changes, describe how changes are enforced, and identify who changes the passwords (the user, the system, or the system administrator).
- Describe how the access control mechanism support individual accountability and audit trails (e.g., passwords are associated with a user ID that is assigned to a single person).
- Describe the self-protection techniques for the user authentication mechanism (passwords are encrypted, automatically generated, are checked against a dictionary of disallowed passwords, passwords are encrypted while in transmission).
- State the number of invalid access attempts that may occur for a given user id or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).

- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifiers, and group user identifiers) and any compensating controls.
- Describe any use of digital or electronic signatures and the standards used. Discuss the key management procedures for key generation, distribution, storage, and disposal.

6.MA.2 Logical Access Controls

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the application. Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists [ACLs]).
- How are access rights granted? Are privileges granted based on job function?
- Describe the application's capability to establish an ACL or register.
- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
- Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Dept. of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

6.MA.3 Public Access Controls

If the public accesses the major application, discuss the additional security controls used to protect the integrity of the application and the confidence of the public in the application. Such controls include segregating information made directly accessible to the public from official agency records. Others might include:

- Some form of identification and authentication
- Access control to limit what the user can read, write, modify, or delete
- Controls to prevent public users from modifying information on the system
- Digital signatures
- CD-ROM for on-line storage of information for distribution
- Put copies of information for public access on a separate system
- Prohibit public to access live databases

- Verify that programs and information distributed to the public are virus-free
- Audit trails and user confidentiality
- System and data availability
- Legal considerations

6.MA.4 Audit Trails

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (type of event, when the event occurred, user id associated with the event, program or command used to initiate the event.)
- Is access to online audit logs strictly enforced?
- Is the confidentiality of audit trail information protected if, for examples, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are guidelines.
- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.

TABLE A1: CYBER SECURITY POLICY AND DEPARTMENT DIRECTIVES

Guidance/ Directive

Number	Title	Date
CS-002	2001 Annual Information Cyber Security Plan Call	4/10/01
CS-002A	2001 Annual Information Cyber Security Plan Call (Tactical Radio Network Call),	5/17/01
CS-003	USDA Internet Access Security for Private Internet Service Providers,	5/25/01
CS-004	Interim Policy on Reuse of User Logon Identification	5/10/01
CS-005	Interim Guidance on Physical Security in USDA Information Technology (IT) Restricted Space	11/28/01
CS-006	Interim Guidance on USDA Privacy Requirements & the Use of Cookies on Web Pages	5/22/01
CS-007	Interim Guidance on Vulnerability Scan Procedures	9/5/01
CS-008	Interim Guidance Regarding the Use of Public Key Infrastructure (PKI) Technology in USDA	11/28/02
CS-009	Interim Guidance on Configuration Management Part 1	10/16/01
CS-010	Interim Guidance on Peer-to-Peer (P2P) Software and Copyright Protection	1/22/02
CS-011	IBM & IBM Compatible Security Standards	12/4/01
CS-012	Cyber Security Guidance Regarding Gateway and Technical Security Standards	1/22/02
CS-013	Cyber Security Guidance Regarding C2 Controlled Access Protection	3/7/02
CS-014	Cyber Security Guidance Regarding 2002 Annual Agency Information Cyber Security Plan Call	5/8/02
CS-015	Cyber Security Guidance Regarding Computer Security Awareness Training Programs	4/3/02
CS-016	Cyber Security Guidance Regarding Risk Assessments and Security Checklists	7/19/02
CS-017	Required Language for Agency Warning Banners	11/13/02
CS-018	Cyber Security Guidance Memos	10/3/02
CS-019	Cyber Security Guidance Regarding Privacy Impact Assessments	11/13/02
CS-020	Cyber Security Guidance Regarding Waiver Requests	12/20/02
DM 3500	Chapter 1, USDA Computer Incident Response	10/25/01
DR 3140-1	USDA ADP Security Policy	5/15/96
DR 3140-2	USDA Internet Security Policy	3/7/95

TABLE A2: LEVELS OF CONCERN FOR SYSTEM CRITICALITY/SENSITIVITY

	LOW	MODERATE	HIGH
CONFIDENTIALITY SENSITIVE INFORMATION (UNCLASSIFIED)	The consequences of unauthorized disclosure or compromise of data or information in the system are **generally acceptable**. Loss of confidentiality could be expected to affect agency-level interests and have some negative impact on mission accomplishment.	The consequences of unauthorized disclosure or compromise of data or information in the system are only **marginally acceptable**. Loss of confidentiality could be expected to adversely affect agency-level interests degrade mission accomplishment or create unsafe conditions that may result in injury or serious damage.	The consequences of unauthorized disclosure or compromise of data or information in the system are **unacceptable**. Loss of confidentiality could be expected to adversely affect national-level interests, prevent mission accomplishment or create unsafe conditions that may result in loss of life or other exceptionally grave damage.
CONFIDENTIALITY NATIONAL SECURITY INFORMATION (CLASSIFIED)	Not applicable.	Not applicable.	The consequences of unauthorized disclosure or compromise of data or information in the system are **unacceptable**. Loss of confidentiality could be expected to cause exceptionally grave damage, serious damage, or damage to the national security.
INTEGRITY	The consequences of corruption or unauthorized modification of data or information in the system are **generally acceptable**. Loss of integrity could be expected to affect agency-level interests and have some negative impact on mission accomplishment.	The consequences of corruption or unauthorized modification of data or information in the system are only **marginally acceptable**. Loss of integrity could be expected to adversely affect agency-level interests degrade mission accomplishment or create unsafe conditions that may result in injury or serious damage.	The consequences of corruption or unauthorized modification of data or information in the system are **unacceptable**. Loss of integrity could be expected to adversely affect national-level interests, prevent mission accomplishment or create unsafe conditions that may result in loss of life or other exceptionally grave damage.
AVAILABILITY	The consequences of loss or disruption of access to system resources or to data or information in the system are **generally acceptable**. Loss of availability could be expected to affect agency-level interests and have some negative impact on mission accomplishment.	The consequences of loss or disruption of access to system resources or to data or information in the system are only **marginally acceptable**. Loss of availability could be expected to adversely affect agency-level interests, degrade mission accomplishment or create unsafe conditions that may result in injury or serious damage.	The consequences of loss or disruption of access to system resources or to data or information in the system are **unacceptable**. Loss of availability could be expected to adversely affect national-level interests, prevent mission accomplishment or create unsafe conditions that may result in loss of life or other exceptionally grave damage.